

SOME FINITE ABELIAN GROUP THEORY AND SOME  $q$ -SERIES IDENTITIES

DEREK GARTON

## 1. INTRODUCTION

In 1984, Cohen and Lenstra [CL84] famously presented a family of conjectures about the structure of ideal class groups of number fields. These conjectures follow from this heuristic:

**Heuristic 1.1.** *For any odd prime  $\ell$ , a finite abelian  $\ell$ -group should appear as the  $\ell$ -Sylow subgroup of the ideal class group of an imaginary quadratic extension of  $\mathbb{Q}$  with frequency inversely proportional to the order of its automorphism group.*

Their heuristic leads to a probability distribution on the poset of isomorphism classes of finite abelian  $\ell$ -groups. They computed various averages on this poset using this distribution, averages that lead directly to their conjectures. Along the way, they proved a variety of identities concerning finite abelian  $\ell$ -groups, such as the identity of Hall [Hal38], which shows that their heuristic does indeed give a probability distribution:

$$\sum_{\substack{\text{finite abelian} \\ \ell\text{-groups } A}} \frac{1}{|\text{Aut } A|} = \prod_{i=1}^{\infty} (1 - \ell^{-i})^{-1}.$$

More recently, Delaunay and Delaunay-Jouhet ([Del11],[DJ14],[DJ]) computed new averages using this distribution. They proceeded to use these averages to study the structure of Tate-Shafarevich groups and Selmer groups of elliptic curves. Moreover, they showed that the averages they computed are consistent with the conjectures of Poonen-Rains ([PR12]). Like Cohen and Lenstra, they discovered new and interesting identities along the way to computing these averages.

In this paper, we continue the tradition of studying finite abelian group identities to investigate number theoretic phenomena. The simplest identity is Lemma 3.2: for any finite abelian  $\ell$ -group  $A$  of  $\ell$ -rank  $r$ ,

$$\sum_{\substack{\text{finite abelian} \\ \ell\text{-groups } B \\ \text{rank}_{\ell} B = r}} \frac{|\{C \leq B \mid C \simeq A\}|}{|\text{Aut } B|} = \frac{1}{|\text{Aut } A|} \cdot \prod_{i=1}^r (1 - \ell^{-i})^{-1},$$

but see also Corollary 3.5, Lemma 5.3, and Corollary 5.4. These identities are crucial in constructing a random matrix justification for Malle's conjectural distribution of relative ideal class groups of number fields in the presence of unexpected roots of unity (see [Mal08] and [Mal10]). See [Gar14b] for this random matrix construction.

The organization of this paper is as follows. Section 2 contains notation and definitions, Sections 3 and 5 present the averages of finite abelian  $\ell$ -groups, and Section 4 presents two  $q$ -series identities which are important for later computations in this paper.

## 2. NOTATION AND DEFINITIONS

Let  $\ell$  be an odd prime and let  $\mathcal{G}$  be the poset of isomorphism classes of finite abelian  $\ell$ -groups, with the relation  $[A] \leq [B]$  if and only if there exists an injection  $A \hookrightarrow B$ . (For notational simplicity, we will conflate finite abelian  $\ell$ -groups and the equivalence classes containing them.) If  $i \in \mathbb{Z}^{>0}$ , let

$$\text{rank}_{\ell^i} A := \dim_{\mathbb{F}_{\ell}} (\ell^{i-1} A / \ell^i A).$$

We will abbreviate  $\text{rank}_{\ell} A$  by  $\text{rank } A$ .

**Definition 2.1.** For any  $r_1, \dots, r_i \in \mathbb{Z}^{\geq 0}$ , define the following subposet of  $\mathcal{G}$ :

$$\mathcal{G}(r_1, \dots, r_i) := \{A \in \mathcal{G} \mid \text{rank}_{\ell^j}(A) = r_j \text{ for all } 1 \leq j \leq i\}.$$

Next, we define a function  $S : \mathcal{G} \times \mathcal{G} \rightarrow \mathbb{Z}$  that is related to the Möbius function on  $\mathcal{G}$ . See [Gar14a] for a deeper discussion of this relationship.

**Definitions 2.2.** For any  $A, B \in \mathcal{G}$ , let  $\text{sub}(A, B)$  be the number of subgroups of  $B$  that are isomorphic to  $A$ . If  $A \in \mathcal{G}$ , an  $A$ -chain is a finite (possibly empty) linearly ordered subset of  $\{B \in \mathcal{G} \mid B > A\}$ . Now, given an  $A$ -chain  $\mathfrak{C} = \{A_j\}_{j=1}^i$ , define

$$\text{sub}(\mathfrak{C}) := (-1)^i \text{sub}(A, A_1) \prod_{j=1}^{i-1} \text{sub}(A_j, A_{j+1}).$$

(We set  $\text{sub}(\mathfrak{C}) = 1$  if  $\mathfrak{C}$  is empty.) Finally, for any  $A, B \in \mathcal{G}$ , let

$$S(A, B) = \begin{cases} 0 & \text{if } A \not\leq B, \\ 1 & \text{if } A = B, \\ \sum_{\substack{A\text{-chains } \mathfrak{C}, \\ \max \mathfrak{C} = B}} \text{sub}(\mathfrak{C}) & \text{if } A < B. \end{cases}$$

The definitions that follow are standard in the study of  $q$ -series.

**Notation 2.3.** For  $q, z \in \mathbb{C}$  with  $|q| < 1$  and any  $i \in \mathbb{Z}^{\geq 0}$ , let

$$(z; q)_i := \prod_{j=0}^{i-1} (1 - q^j z).$$

To ease notation, set  $(q)_i := (q; q)_i$ . Next, we define the  $q$ -binomial coefficients: for any  $k, m \in \mathbb{Z}^{\geq 0}$ , let

$$\binom{k}{m}_q := \frac{(q)_k}{(q)_m (q)_{k-m}},$$

with  $\binom{k}{m}_q := 0$  if  $k < m$ .

In Sections 3 and 5, we will set  $q = 1/\ell$ , but the results in Section 4 hold for any complex number  $q$  of modulus less than 1.

### 3. SOME IDENTITIES FROM FINITE ABELIAN GROUP THEORY

Before proving the first identity, we will follow [CL84] and [Hal38] in making two more definitions, which we will use only in the proof of Lemma 3.2. In this section, we set  $q = 1/\ell$ .

**Definition 3.1.** For any  $A \in \mathcal{G}$  and  $i \in \mathbb{Z}^{\geq 0}$ , define the  $i$ -weight of  $A$  to be

$$w_i(A) := \frac{|\text{Surj}(\mathbb{Z}^i, A)|}{|A|^i |\text{Aut } A|},$$

and for any  $j \in \mathbb{Z}^{\geq 0}$ , define

$$w_i(\ell^j) := \sum_{\substack{A \in \mathcal{G} \\ |A| = \ell^j}} w_i(A).$$

**Lemma 3.2.** Suppose that  $A \in \mathcal{G}$  and  $\text{rank } A = r$ . Then

$$\sum_{B \in \mathcal{G}(r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} = \frac{1}{(q)_r |\text{Aut } A|}.$$

*Proof.* By Proposition 3.1 of [CL84], we know

$$\sum_{B \in \mathcal{G}(r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} = \sum_{B \in \mathcal{G}(r)} \frac{w_r(B)}{(q)_r} \text{sub}(A, B).$$

Next, we will simplify this summation by making two complementary observations concerning any  $B \in \mathcal{G}$ . First, if  $\text{rank } B > r$ , then  $w_r(B) = 0$  by the definition of the  $r$ -weight of  $G$ . Second, if  $\text{rank } B < r$ , then  $\text{sub}(A, B) = 0$ . Thus, our sum becomes

$$\begin{aligned} \sum_{B \in \mathcal{G}(r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} &= \frac{1}{(q)_r} \cdot \sum_{B \in \mathcal{G}} w_r(B) \text{sub}(A, B) \\ &= \frac{1}{(q)_r} \cdot \sum_{i=0}^{\infty} \sum_{\substack{B \in \mathcal{G} \\ |B| = \ell^i}} w_r(B) \text{sub}(A, B). \end{aligned}$$

By Proposition 4.1 of [CL84], if  $\ell^i \geq |A|$ , then

$$\sum_{\substack{B \in \mathcal{G} \\ |B| = \ell^i}} w_r(B) \text{sub}(A, B) = w_r(\ell^i |A|^{-1}) w_r(A).$$

If, on the other hand,  $\ell^i < |A|$ , then the above sum clearly vanishes. Thus,

$$\sum_{B \in \mathcal{G}(r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} = \frac{1}{(q)_r} \cdot w_r(A) \cdot \sum_{i=0}^{\infty} w_r(\ell^i).$$

Finally, we apply Proposition 3.1 (again) and Corollary 3.7 of [CL84] to obtain

$$\sum_{B \in \mathcal{G}(r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} = \frac{1}{(q)_r} \cdot \frac{(q)_r}{|\text{Aut } A|} \cdot \frac{1}{(q)_r},$$

as desired. □

Before our next result, we need a few more definitions.

**Definitions 3.3.** For any  $A \in \mathcal{G}$  and any  $A$ -chain  $\mathfrak{C} = \{A_j\}_{j=1}^i$ , define

$$\text{sub}_+(\mathfrak{C}) := \text{sub}(A, A_1) \prod_{j=1}^{i-1} \text{sub}(A_j, A_{j+1}).$$

If  $A, B \in \mathcal{G}$ , let

$$S_+(A, B) := \begin{cases} 0 & \text{if } A \not\leq B, \\ 1 & \text{if } A = B, \\ \sum_{\substack{A\text{-chains } \mathfrak{C}, \\ \max \mathfrak{C} = B}} \text{sub}_+(\mathfrak{C}) & \text{if } A < B. \end{cases}$$

Finally, suppose  $A \in \mathcal{G}(r)$  for some  $r \in \mathbb{Z}^{\geq 0}$ . Then for any  $i \in \mathbb{Z}^{\geq 0}$ , let

$$\varsigma_i(A) := \sum_{\substack{A\text{-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r) \\ |\mathfrak{C}| = i}} \frac{\text{sub}_+(\mathfrak{C})}{|\text{Aut}(\max \mathfrak{C})|}.$$

We know that  $\varsigma_i(A)$  converges by the following lemma.

**Lemma 3.4.** *If  $A \in \mathcal{G}(r)$  for some  $r \in \mathbb{Z}^{\geq 0}$ , and  $i \in \mathbb{Z}^{\geq 0}$ , then*

$$\varsigma_i(A) = \frac{((q)_r^{-1} - 1)^i}{|\text{Aut } A|}.$$

*Proof.* We will induct on  $i$ . Note that the case  $i = 0$  is trivially true and the case  $i = 1$  is true by [Lemma 3.2](#). Using the induction hypothesis and [Lemma 3.2](#), we see that for any  $i \geq 1$ ,

$$\begin{aligned}
\varsigma_i(A) &= \sum_{\substack{A\text{-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r) \\ |\mathfrak{C}|=i}} \frac{\text{sub}_+(\mathfrak{C})}{|\text{Aut}(\max \mathfrak{C})|} \\
&= \sum_{\substack{A\text{-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r) \\ |\mathfrak{C}|=i-1}} \text{sub}_+(\mathfrak{C}) \cdot \sum_{\substack{B \in \mathcal{G}(r) \\ B \neq \max \mathfrak{C}}} \frac{\text{sub}(\max \mathfrak{C}, B)}{|\text{Aut } B|} \\
&= \sum_{\substack{A\text{-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r) \\ |\mathfrak{C}|=i-1}} \text{sub}_+(\mathfrak{C}) \cdot \frac{(q)_r^{-1} - 1}{|\text{Aut}(\max \mathfrak{C})|} \\
&= \frac{((q)_r^{-1} - 1)^i}{|\text{Aut } A|},
\end{aligned}$$

as desired. □

**Corollary 3.5.** *If  $A \in \mathcal{G}(r)$  for some  $r \in \mathbb{Z}^{\geq 0}$ , then*

$$\sum_{B \in \mathcal{G}(r)} \frac{S(A, B)}{|\text{Aut } B|} = \frac{(q)_r}{|\text{Aut } A|}.$$

*Proof.* Since  $\ell$  is odd, we know that  $0 < (q)_r^{-1} - 1 < 1$ . Moreover,

$$\sum_{B \in \mathcal{G}(r)} \frac{S(A, B)}{|\text{Aut } B|} = \sum_{i=0}^{\infty} (-1)^i \varsigma_i(A).$$

□

**Corollary 3.6.** *f  $A \in \mathcal{G}(r)$  for some  $r \in \mathbb{Z}^{\geq 0}$ , then*

$$\sum_{B \in \mathcal{G}(r)} \frac{S_+(A, B)}{|\text{Aut } B|} = \frac{(q)_r}{(2(q)_r - 1) |\text{Aut } A|}.$$

#### 4. TWO $q$ -SERIES IDENTITIES

We record here two  $q$ -series identities that we will need in [Section 5](#). The first follows from the  $q$ -binomial theorem, and the second follows from the  $q$ -Chu-Vandermonde sum. In this section, we allow  $q$  to be any complex number of modulus less than 1.

**Corollary 4.1.** *Suppose that  $k \in \mathbb{Z}^{> 0}$ . Then*

$$\sum_{i=0}^k (-1)^i \binom{k}{i}_q q^{\frac{i(i+1)}{2} - ik} = 0.$$

*Proof.* We use the following corollary of the  $q$ -binomial theorem: for any  $z \in \mathbb{C}$ ,

$$\sum_{i=0}^k (-1)^i \binom{k}{i}_q q^{\frac{i(i-1)}{2}} z^i = (z; q)_k.$$

This is given as Corollary 10.2.2 (part (c)) in [\[AAR99\]](#) (though, as the authors mention, it is due to Rothe). We substitute  $x = -q^{-k+1}$  to obtain the result. □

**Corollary 4.2.** *Suppose that  $m, k \in \mathbb{Z}^{\geq 0}$ . Then*

$$\sum_{i=0}^{\infty} \binom{m}{i}_q \binom{k}{i}_q (q)_i q^{(m-i)(k-i)} = 1.$$

*Proof.* Using the standard notation for hypergeometric functions, note that

$$\sum_{i=0}^{\infty} \binom{m}{i}_q \binom{k}{i}_q (q)_i q^{(m-i)(k-i)} = q^{mk} \cdot {}_2\phi_1(q^{-m}, q^{-k}; 0; q, q).$$

The result then follows from the  $q$ -Chu-Vandermonde sum, which states that

$${}_2\phi_1(a, q^{-n}; c; q, q) = \frac{(\frac{c}{a}; q)_n}{(c; q)_n} a^n;$$

see Formula II.6 from Appendix II in [GR04].  $\square$

## 5. MORE IDENTITIES FROM FINITE ABELIAN GROUP THEORY

Before continuing, we need one more bit of notation and a lemma that follows from work in [Gar14a]. In this section, we once again set  $q = 1/\ell$ .

**Notation 5.1.** For any  $A \in \mathcal{G}$  and any  $i \in \mathbb{Z}^{\geq 0}$ , let

$$A_{\oplus i} := A \oplus \overbrace{(\mathbb{Z}/\ell) \oplus \cdots \oplus (\mathbb{Z}/\ell)}^{i \text{ times}}.$$

**Lemma 5.2.** If  $s, i \in \mathbb{Z}^{\geq 0}$  and  $A \in \mathcal{G}(s, s)$ , then

$$|\text{Aut } A_{\oplus i}| = q^{-i(2s+i)} (q)_i |\text{Aut } A|.$$

*Proof.* Computation following from Theorem 2.2 in [Gar14a].  $\square$

**Lemma 5.3.** Suppose  $r, s \in \mathbb{Z}^{\geq 0}$  and  $r \geq s$ . If  $A \in \mathcal{G}(r, s)$  and  $i \in \{s, \dots, r\}$ , then

$$\sum_{B \in \mathcal{G}(r, i)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} = \binom{r-s}{r-i}_q \cdot \frac{q^{i(i-s)}}{(q)_i |\text{Aut } A|}.$$

*Proof.* We begin by considering the  $i = r$  case, which we will prove by induction on  $r - s$ . (When  $r - s = 0$ , the  $i = r$  case is clearly true by Lemma 3.2.) Now, there exists a unique  $A_0 \in \mathcal{G}(s, s)$  such that  $A = (A_0)_{\oplus(r-s)}$ . Next, by Lemma 3.2, Lemma 5.2 (twice), Lemma 2.5 of [Gar14a], and the induction hypothesis, we see that

$$\begin{aligned} \frac{1}{(q)_r |\text{Aut } A|} &= \sum_{B \in \mathcal{G}(r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} \\ &= \sum_{j=s}^r \sum_{B \in \mathcal{G}(r, j)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} \\ &= \sum_{j=s}^r \sum_{B \in \mathcal{G}(j, j)} \frac{q^{(r-j)(r+j)} \text{sub}((A_0)_{\oplus(j-s)}, B)}{(q)_{r-j} |\text{Aut } B|} \\ &= \sum_{j=s}^{r-1} \frac{q^{(r-j)(r+j)} \cdot q^{j(j-s)}}{(q)_{r-j} \cdot (q)_j |\text{Aut } (A_0)_{\oplus(j-s)}|} + \sum_{B \in \mathcal{G}(r, r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} \\ &= \sum_{j=s}^{r-1} \frac{q^{(r-j)(r+j)} \cdot q^{j(j-s)} \cdot q^{(j-s)(j+s)} (q)_{r-s}}{(q)_{r-j} \cdot (q)_j \cdot q^{(r-s)(r+s)} (q)_{j-s} |\text{Aut } A|} + \sum_{B \in \mathcal{G}(r, r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} \\ &= \frac{1}{|\text{Aut } A|} \cdot \sum_{j=s}^{r-1} \binom{r-s}{r-j}_q \cdot \frac{q^{j(j-s)}}{(q)_j} + \sum_{B \in \mathcal{G}(r, r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} \end{aligned}$$

Letting  $m = r - s$ , we obtain

$$\frac{1}{(q)_r |\text{Aut } A|} = \frac{1}{|\text{Aut } A|} \cdot \sum_{j=0}^{m-1} \binom{m}{m-j}_q \cdot \frac{q^{j(r+j-m)}}{(q)_{r+j-m}} + \sum_{B \in \mathcal{G}(r, r)} \frac{\text{sub}(A, B)}{|\text{Aut } B|}.$$

Thus,

$$\begin{aligned}
\sum_{B \in \mathcal{G}(r,r)} \frac{\text{sub}(A,B)}{|\text{Aut } B|} &= \frac{1}{(q)_r |\text{Aut } A|} \cdot \left( 1 - \sum_{j=0}^{m-1} \binom{m}{m-j}_q \cdot \frac{q^{j(r+j-m)} (q)_r}{(q)_{r+j-m}} \right) \\
&= \frac{1}{(q)_r |\text{Aut } A|} \cdot \left( 1 - \sum_{j=0}^{m-1} \binom{m}{j}_q \binom{r}{m-j}_q \cdot (q)_{m-j} q^{j(r+j-m)} \right) \\
&= \frac{1}{(q)_r |\text{Aut } A|} \cdot \left( 1 - \sum_{j=1}^m \binom{m}{j}_q \binom{r}{j}_q \cdot (q)_j q^{(m-j)(r-j)} \right) \\
&= \frac{1}{(q)_r |\text{Aut } A|} \cdot (1 - (1 - q^{mr})) \quad (\text{by Corollary 4.2}) \\
&= \frac{q^{r(r-s)}}{(q)_r |\text{Aut } A|},
\end{aligned}$$

concluding the  $i = r$  case.

For the general case, the same techniques as above show that

$$\begin{aligned}
\sum_{B \in \mathcal{G}(r,i)} \frac{\text{sub}(A,B)}{|\text{Aut } A|} &= \sum_{B \in \mathcal{G}(i,i)} \frac{q^{(r-i)(r+i)} \text{sub}((A_0)_{\oplus(i-s)}, B)}{(q)_{r-i} |\text{Aut } B|} \\
&= \frac{q^{(r-i)(r+i)} \cdot q^{i(i-s)}}{(q)_{r-i} \cdot (q)_i |\text{Aut } (A_0)_{\oplus(i-s)}|} \\
&= \frac{q^{(r-i)(r+i)} \cdot q^{i(i-s)} \cdot q^{(i-s)(i+s)} (q)_{r-s}}{(q)_{r-i} \cdot (q)_i \cdot q^{(r-s)(r+s)} (q)_{i-s} |\text{Aut } A|},
\end{aligned}$$

completing the proof. □

**Corollary 5.4.** *Suppose  $r, s \in \mathbb{Z}^{\geq 0}$  and  $r \geq s$ . If  $A \in \mathcal{G}(r, s)$  and  $i \in \{s, \dots, r\}$ , then*

$$\sum_{B \in \mathcal{G}(r,i)} \frac{S(A,B)}{|\text{Aut } B|} = (-1)^{i-s} q^{\frac{i(i+1)}{2} - \frac{s(s+1)}{2}} \cdot \binom{r-s}{r-i}_q \cdot \frac{(q)_s}{|\text{Aut } A|}.$$

*Proof.* Throughout this proof, we will rearrange terms of infinite alternating sums. The fact that we can do so follows from Corollary 3.6. To ease notation, let

$$X_i := \sum_{B \in \mathcal{G}(r,i)} \frac{S(A,B)}{|\text{Aut } B|}.$$

As a first step toward the the result, we claim that

$$X_i = \begin{cases} \frac{(q)_s}{|\text{Aut } A|} & \text{if } i = s \\ - \sum_{j=s}^{i-1} q^{i(i-j)} \cdot \binom{r-j}{r-i}_q \cdot X_j & \text{if } i > s. \end{cases}$$

If  $i = s$ , we use [Lemma 3.2](#) to obtain:

$$\begin{aligned}
X_s &= \sum_{j=0}^{\infty} \sum_{\substack{\text{A-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r,s) \\ |\mathfrak{C}|=j}} \left( \frac{\text{sub}(\mathfrak{C})}{|\text{Aut}(\max \mathfrak{C})|} \right) \\
&= \frac{1}{|\text{Aut } A|} - \sum_{j=1}^{\infty} \sum_{\substack{\text{A-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r,s) \\ |\mathfrak{C}|=j-1}} \text{sub}(\mathfrak{C}) \cdot \sum_{\substack{B \in \mathcal{G}(r,s) \\ B \neq \max \mathfrak{C}}} \left( \frac{\text{sub}(\max \mathfrak{C}, B)}{|\text{Aut } B|} \right) \\
&= \frac{1}{|\text{Aut } A|} - \left( \frac{1}{(q)_s} - 1 \right) \sum_{j=1}^{\infty} \sum_{\substack{\text{A-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r,s) \\ |\mathfrak{C}|=j-1}} \frac{\text{sub}(\mathfrak{C})}{|\text{Aut}(\max \mathfrak{C})|} \\
&= \frac{1}{|\text{Aut } A|} - \left( \frac{1}{(q)_s} - 1 \right) X_s.
\end{aligned}$$

The result follows by solving for  $X_s$ . If, on the other hand,  $i > s$ , we can apply [Lemma 5.3](#) to see that

$$\begin{aligned}
X_i &= \sum_{k=1}^{\infty} \sum_{\substack{\text{A-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r,i) \\ |\mathfrak{C}|=k}} \left( \frac{\text{sub}(\mathfrak{C})}{|\text{Aut}(\max \mathfrak{C})|} \right) \\
&= - \sum_{B \in \mathcal{G}(r,i)} \frac{\text{sub}(A, B)}{|\text{Aut } B|} - \sum_{j=s}^{i-1} \sum_{k=2}^{\infty} \sum_{\substack{\text{A-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r,j) \\ |\mathfrak{C}|=k-1}} \text{sub}(\mathfrak{C}) \cdot \sum_{B \in \mathcal{G}(r,i)} \frac{\text{sub}(\max \mathfrak{C}, B)}{|\text{Aut } B|} \\
&\quad - \sum_{k=2}^{\infty} \sum_{\substack{\text{A-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r,i) \\ |\mathfrak{C}|=k-1}} \text{sub}(\mathfrak{C}) \cdot \sum_{\substack{B \in \mathcal{G}(r,i) \\ B \neq \max \mathfrak{C}}} \frac{\text{sub}(\max \mathfrak{C}, B)}{|\text{Aut } B|} \\
&= - \binom{r-s}{r-i}_q \cdot \frac{q^{i(i-s)}}{(q)_i |\text{Aut } A|} - \sum_{j=s}^{i-1} \binom{r-j}{r-i}_q \cdot \frac{q^{i(i-j)}}{(q)_i} \cdot \sum_{k=2}^{\infty} \sum_{\substack{\text{A-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r,k) \\ |\mathfrak{C}|=k-1}} \frac{\text{sub}(\mathfrak{C})}{|\text{Aut}(\max \mathfrak{C})|} \\
&\quad - \left( \frac{1}{(q)_i} - 1 \right) \sum_{k=2}^{\infty} \sum_{\substack{\text{A-chains } \mathfrak{C} \\ \max \mathfrak{C} \in \mathcal{G}(r,k) \\ |\mathfrak{C}|=k-1}} \frac{\text{sub}(\mathfrak{C})}{|\text{Aut}(\max \mathfrak{C})|} \\
&= - \sum_{j=s}^{i-1} \left( \binom{r-j}{r-i}_q \cdot \frac{q^{i(i-j)}}{(q)_i} \cdot X_j \right) - \left( \frac{1}{(q)_i} - 1 \right) X_i.
\end{aligned}$$

The claim follows by solving for  $X_i$ .

By the claim above, the lemma is true for  $i = s$ ; we will now prove the lemma by induction on  $i$ . Using the induction hypothesis, note that

$$\begin{aligned}
X_i &= - \sum_{j=s}^{i-1} q^{i(i-j)} \cdot \binom{r-j}{r-i}_q \cdot X_j \\
&= - \sum_{j=s}^{i-1} \frac{q^{i(i-j)}}{(q)_{r-i}(q)_{i-j}} \cdot \frac{(-1)^{j-s} q^{\frac{i(j+1)}{2}} (q)_{r-s} (q)_s}{q^{\frac{s(s+1)}{2}} (q)_{j-s} |\text{Aut } A|} \\
&= - \frac{(q)_{r-s} (q)_s}{q^{\frac{s(s+1)}{2}} (q)_{r-i} |\text{Aut } A|} \cdot \sum_{j=s}^{i-1} \frac{(-1)^{j-s} q^{i(i-j) + \frac{j(j+1)}{2}}}{(q)_{i-j} (q)_{j-s}} \\
&= - \frac{(q)_{r-s} (q)_s}{q^{\frac{s(s+1)}{2}} (q)_{r-i} |\text{Aut } A|} \cdot \sum_{j=0}^{i-s-1} \frac{(-1)^j q^{i(i-j-s) + \frac{(j+s)(j+s+1)}{2}}}{(q)_{i-j-s} (q)_j}.
\end{aligned}$$

Letting  $k = i - s$ , and using [Corollary 4.1](#), we see that

$$\begin{aligned} X_i &= -\frac{q^{ik}(q)_{r-s}(q)_s}{(q)_{r-i} |\text{Aut } A|} \cdot \sum_{j=0}^{k-1} (-1)^j \frac{q^{\frac{i(j+1)}{2}-jk}}{(q)_{k-j}(q)_j} \\ &= -\frac{q^{ik}(q)_{r-s}(q)_s}{(q)_{r-i} |\text{Aut } A|} \cdot \left( -(-1)^k \frac{q^{\frac{k(k+1)}{2}-k^2}}{(q)_k} \right). \end{aligned}$$

Substituting for  $k$  gives the result. □

## REFERENCES

- [AAR99] George E. Andrews, Richard Askey, and Ranjan Roy, [Special functions](#), Encyclopedia of Mathematics and its Applications, vol. 71, Cambridge University Press, Cambridge, 1999. MR 1688958 (2000g:33001)
- [CL84] H. Cohen and H. W. Lenstra, Jr., [Heuristics on class groups of number fields](#), Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62. MR 756082 (85j:11144)
- [Del11] Christophe Delaunay, [Averages of groups involving  \$p^\ell\$ -rank and combinatorial identities](#), J. Number Theory **131** (2011), no. 3, 536–551. MR 2741224 (2011k:11153)
- [DJ] C. Delaunay and F. Jouhet, [The Cohen-Lenstra heuristics, moments and  \$p^j\$ -ranks of some groups](#), To appear in *Acta Arith.*
- [DJ14] Christophe Delaunay and Frédéric Jouhet,  [\$p^\ell\$ -torsion points in finite abelian groups and combinatorial identities](#), Adv. Math. **258** (2014), 13–45. MR 3190422
- [Gar14a] D. Garton, [A weighted Möbius function](#), ArXiv e-prints (2014).
- [Gar14b] ———, [Random matrices, the Cohen-Lenstra heuristics, and roots of unity](#), ArXiv e-prints (2014).
- [GR04] George Gasper and Mizan Rahman, [Basic hypergeometric series](#), second ed., Encyclopedia of Mathematics and its Applications, vol. 96, Cambridge University Press, Cambridge, 2004, With a foreword by Richard Askey. MR 2128719 (2006d:33028)
- [Hal38] P. Hall, [A partition formula connected with Abelian groups](#), Comment. Math. Helv. **11** (1938), no. 1, 126–129. MR 1509594
- [Mal08] Gunter Malle, [Cohen-Lenstra heuristic and roots of unity](#), J. Number Theory **128** (2008), no. 10, 2823–2835. MR 2441080 (2009j:11179)
- [Mal10] ———, [On the distribution of class groups of number fields](#), Experiment. Math. **19** (2010), no. 4, 465–474. MR 2778658
- [PR12] Bjorn Poonen and Eric Rains, [Random maximal isotropic subspaces and Selmer groups](#), J. Amer. Math. Soc. **25** (2012), no. 1, 245–269. MR 2833483